AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

Claim 1 (Currently Amended): A method ~~for operating a computer~~ comprising:

sensing whether a storage device has device-specific security information stored thereon;

operating ~~the~~ a computer in a full-access mode when the storage device has the device-specific security information, wherein in the full-access mode the computer permits both read and write access to the storage device; and

operating the computer in a restricted-access mode when the storage device does not have the device-specific security information, wherein in the restricted-access mode the computer permits read access to the storage device and prevents write access to the storage device.

Claim 2 (Currently Amended): The method of claim 1, wherein operating the computer in a full-access mode includes automatically encrypting and decrypting a data stream between the computer and the storage device by ~~the following~~:

encrypting digital data to be written to the storage ~~disk~~ device from the computer; and

decrypting digital data read from the storage device by the computer.

Claim 3 (Original): The method of claim 2, wherein the digital data is encrypted and decrypted using a cryptographic key generated from format information for the storage device.

Claim 4 (Original): The method of claim 2, wherein the digital data is encrypted and decrypted using a cryptographic key generated from information etched on the storage device during manufacturing.

PAGE 3/22 * RCVD AT 2/16/2004 3:10:12 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-2/0 * DNIS:7465447 * CSID:651 704 5951 * DURATION (mm-ss):07-14

Claim 5 (Original): The method of claim 2, wherein the digital data is encrypted and decrypted using a cryptographic key generated from information specific to a removable media drive used for accessing the storage device.

Claim 6 (Original): The method of claim 5, wherein the drive-specific information includes a drive serial number.

Claim 7 (Original): The method of claim 5, wherein the drive-specific information includes calibration parameters for the drive.

Claim 8 (Cancelled).

Claim 9 (Currently Amended): The method of claim 1, wherein operating the computer in [[a]] the full-access mode includes permitting ~~the~~ a user to access sensitive data stored on a remote computer.

Claim 10 (Currently Amended): The method of claim 1, wherein operating the computer in [[a]] the full-access mode includes permitting the user to access a second storage device.

Claim 11 (Currently Amended): The method of claim 10, wherein operating the computer in [[a]] the full-access mode includes decrypting digital data read from a second storage device using a cryptographic key generated from the device-specific security information.

Claim 12 (Original): The method of claim 1, wherein sensing the storage device is performed when a status change is detected for the storage device.

Claim 13 (Original): The method of claim 12, wherein the status change indicates the insertion of the storage device into the computer.

PAGE 4/22 * RCVD AT 2/16/2004 3:10:12 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-2/0 * DNIS:7465447 * CSID:651 704 5951 * DURATION (mm-ss):07-14

Claim 14 (Original): The method of claim 2, wherein the digital data is encrypted and decrypted using a cryptographic key generated from security information written to the storage device during low-level formatting.

Claim 15 (Original): The method of claim 2, wherein the digital data is encrypted and decrypted using a cryptographic key generated from a unique identifier stored within an electronic circuit embedded within the storage device.

Claim 16 (Currently Amended): A method for accessing a storage device comprising:

detecting a storage device within the storage drive;

sensing whether a storage device has device-specific security information stored thereon; ~~and~~

providing full-access to the storage device ~~performing at least the following~~ when the storage device has the device-specific security information by:

encrypting digital data using the security information during a write access to write the digital data to the storage device;, and

decrypting digital data using the security information during a read access to read the digital data from the storage device; and

providing restricted-access to the storage device when the storage device does not store the device-specific security information by preventing the digital data from being written to the storage device during the write access.

Claim 17 (Original): The method of claim 16, wherein encrypting the digital data includes generating a cryptographic key as a function of format characteristics of an underlying storage medium of the storage device.

Claim 18 (Original): The method of claim 16, wherein encrypting the digital data includes generating a cryptographic key as a function of a unique identifier stored within an electronic circuit embedded within the storage device.

PAGE 5/22 * RCVD AT 2/16/2004 3:10:12 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-2/0 * DNIS:7465447 * CSID:651 704 5951 * DURATION (mm-ss):07-14

Claim 19 (Cancelled).

Claim 20 (Currently Amended): A method for controlling accessing to a storage device comprising:

detecting a storage device within a the storage drive;

sensing whether the a storage device has device-specific security information stored thereon generated from a combination of device-specific information associated with the storage device and user-specific information associated with a user;

configuring the storage drive to prevent write access to the storage device when the security information is not sensed; and

configuring the storage drive to permit write access by encrypting digital data using the device-specific security information and writing the encrypted digital data to the storage device when the storage device has the device-specific security information is sensed; and

writing the encrypted digital data to the storage device.

Claim 21 (Currently Amended): The method of claim 20, wherein encrypting digital data using the device-specific security information comprises generating a cryptographic key as a function of low-level format information for the storage device.

Claim 22 (Currently Amended): The method of claim 20[[1]], wherein encrypting digital data using the device-specific security information includes generating a the cryptographic key as a function of the user-specific security information.

Claim 23 (Currently Amended): The method of claim 20[[2]], wherein the user-specific security information is a password.

Claim 24 (Currently Amended): The method of claim 20[[2]], wherein the user-specific security information is biometric information.

Claim 25 (Currently Amended): The method of claim 24, wherein the ~~biometic~~ biometric information is digital output from a retina scanner or a fingerprint scan.

Claim 26 (Original): The method of claim 21, wherein the format information includes a primary defect list.

Claim 27 (Original): The method of claim 21, wherein the format information includes one or more logical block addresses.

Claim 28 (Original): The method of claim 21, wherein generating the key includes computing an arithmetic sum of the format information.

Claim 29 (Original): The method of claim 21, wherein generating the key includes evaluating a polynomial using the format information as data for the polynomial.

Claim 30 (Original): The method of claim 20, wherein writing the encrypted digital data includes writing the encrypted digital data to a removable storage medium.

Claim 31 (Original): The method of claim 30, wherein writing the encrypted digital data includes writing the encrypted digital data to a data storage diskette.

Claim 32 (Currently Amended): A method for securely accessing a storage device within a storage drive comprising:

retrieving drive-specific information from the storage drive and device-specific information from a storage device;

generating a cryptographic key as a function of the drive-specific information and the device-specific information; and

configuring the storage drive to automatically provide full-access to the storage device by:

(a) during a write access to the storage device, encrypting data using the cryptographic key and writing the encrypted data to the storage device via the storage drive[[;]], and

(b) during a read access to the storage device, reading encrypted data from the storage device and decrypting the data using the cryptographic key.

Claim 33 (Original): The method of claim 32, wherein the drive-specific information includes a drive serial number.

Claim 34 (Original): The method of claim 32, wherein the drive-specific information includes calibration parameters for the drive.

Claim 35 (Original): The method of claim 34, wherein the calibration parameters includes configuration parameters for read and write circuitry internal to the storage device.

Claim 36 (Original): The method of claim 35, wherein the calibration parameters are selected from the following set of calibration parameters for the storage drive: tracking parameters, a read channel boost, frequency cutoff values, read threshold values, alignment values, optical alignment correction factors and analog to digital conversion calibrations.

Claim 37 (Currently Amended): A method for securely accessing a plurality of storage devices ~~within a storage drive~~ comprising:

retrieving format information from a first storage device;

retrieving format information from a second storage device; ~~and~~

generating a cryptographic key as a function of the format information for the first storage device and the format information for the second storage device; and

controlling access to the first and second storage devices with the cryptographic key.

PAGE 8/22 * RCVD AT 2/16/2004 3:10:12 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-2/0 * DNIS:7465447 * CSID:651 704 5951 * DURATION (mm-ss):07-14

Claim 38 (Currently Amended): The method of claim 37, ~~and further including~~ wherein controlling accesses further includes:

encrypting data using the cryptographic key during a write access to either the first storage device or the second storage device; and

reading encrypted data and decrypting the read data using the cryptographic key during a read access to either the first storage device or the second storage device.

Claim 39 (Currently Amended): A method for operating a storage drive comprising:

configuring the storage drive to operate in a read-only mode upon power-up;

determining whether ~~the~~ a storage device has device-specific security information written thereon; and

configuring the storage drive to operate in a read/write mode when the storage device within the storage drive has device-specific security information written thereon.

Claim 40 (Currently Amended): The method of claim 39 and further including configuring the storage drive to operate in a the read-only mode when the storage device within the storage drive does not have device-specific security information written thereon.

Claim 41 (Currently Amended): The method of claim 39 and further including configuring the storage drive to preventing all read and write access to the storage device when the storage device within the storage drive does not have device-specific security information written thereon.

Claim 42 (Currently Amended): A computer-readable medium having computer-executable instructions for performing the method of:

retrieving drive-specific information from a storage drive and device-specific information from a storage device;

generating a cryptographic key as a function of the drive-specific information and the device-specific information; and

configuring the storage drive to automatically provide full-access to the storage device by:

PAGE 9/22 * RCVD AT 2/16/2004 3:10:12 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-2/0 * DNIS:7465447 * CSID:651 704 5951 * DURATION (mm-ss):07-14

(a) during a write access to the storage device, encrypting data using the cryptographic key and writing the encrypted data to the storage device via the storage drive[[;]], and

(b) during a read access to the storage device, reading encrypted data from the storage device and decrypting the data using the cryptographic key.

Claim 43 (Original): The computer-readable medium of claim 42, wherein the drive-specific information includes a drive serial number.

Claim 44 (Original): The computer-readable medium of claim 42, wherein the drive-specific information includes calibration parameters for the drive.

Claim 45 (Currently Amended): A computer-readable medium having computer-executable instructions for performing the method of:

sensing whether a storage device has security information stored thereon;

operating ~~the~~ a computer in a full-access mode when the storage device has the device-specific security information, wherein in the full-access mode the computer permits both read and write access to the storage device; and

operating the computer in a restricted-access mode when the storage device does not have the device-specific security information, wherein in the restricted-access mode the computer permits read access to the storage device and prevents write access to the storage device.

Claim 46 (Currently Amended): The computer-readable medium of claim 45, wherein operating the computer in a full-access mode includes the following:

encrypting digital data to be written to the storage ~~disk~~drive; and

decrypting digital data read from the storage device.

PAGE 10/22 * RCVD AT 2/16/2004 3:10:12 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-2/0 * DNIS:7465447 * CSID:651 704 5951 * DURATION (mm-ss):07-14

Claim 47 (Original): The computer-readable medium of claim 46, wherein the digital data is encrypted and decrypted using a cryptographic key generated from format information for the storage device.

Claim 48 (Original): The computer-readable medium of claim 46, wherein the digital data is encrypted and decrypted using a cryptographic key generated from information etched into the storage device during manufacturing.

Claim 49 (Original): The computer-readable medium of claim 46, wherein the digital data is encrypted and decrypted using a cryptographic key generated from information specific to a removable media drive used for accessing the storage device.

Claim 50 (Original): The computer-readable medium of claim 46, wherein the digital data is encrypted and decrypted using a cryptographic key generated from information specific to a user.

Claim 51 (Currently Amended): A computer comprising:

a drive for accessing a data storage device having device-specific security information stored thereon; and

a storage manager to selectively configure the ~~computer~~ drive to operate in a full-access mode of operation or a restricted-access mode of operation as a function of the ~~format information and~~ device-specific security information stored on the storage device, wherein in the full-access mode the drive permits both read and write access to the storage device, and in the restricted-access mode the drive permits read access to the storage device and prevents write access to the storage device.

Claim 52 (Currently Amended): The computer of claim 51, wherein the storage manager generates a cryptographic key as a function of the security information and when operating in

PAGE 11/22 * RCVD AT 2/16/2004 3:10:12 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-2/0 * DNIS:7465447 * CSID:651 704 5951 * DURATION (mm-ss):07-14

full-access mode automatically encrypts and decrypts a data stream associated with the read and write access to the storage device ~~decrypts data stored on the storage device~~ using the generated key.

Claim 53 (Original): The computer of claim 51, wherein the drive includes drive-specific information stored in a non-volatile memory, and further wherein the storage manager generates a cryptographic key as a function of the drive-specific information and decrypts data stored on the storage device using the generated key.

Claim 54 (Original): The computer of claim 51, wherein the storage device includes a serial number physically etched onto the storage device during manufacturing, and further wherein the storage manager generates a cryptographic key as a function of the serial number and decrypts data stored on the storage device using the generated key.

Claim 55 (Original): The computer of claim 51, wherein the storage manager generates a cryptographic key as a function of the format information and user-specific information and decrypts data on the storage device using the generated key.

Claim 56 (Original): The computer of claim 51, wherein the format information of the storage device includes a primary defect list.

Claim 57 (Original): The computer of claim 51, wherein the format information of the storage device includes one or more logical block addresses.

Claim 58 (Original): The computer of claim 51, wherein the storage device is a removable storage medium.

PAGE 12/22 * RCVD AT 2/16/2004 3:10:12 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-2/0 * DNIS:7465447 * CSID:651 704 5951 * DURATION (mm-ss):07-14

Claim 59 (Original): The computer of claim 51, wherein the storage device is a data storage diskette.

Claim 60 (Original): The computer of claim 51, wherein the storage device has a disk-shaped storage medium.

Claim 61 (Currently Amended): A computing system comprising:

a first storage device having format information stored thereon;

a second storage device having data stored thereon; and

a software module executing within the computing system, wherein the software module selectively permits access to the data of the second storage device as a function of the format information ~~and security information~~ stored on the first storage device.

Claim 62 (Original): The computing system of claim 61, wherein the first storage device and second storage device are operatively coupled to two different computers that are communicatively coupled via a network.

Claim 63 (Original): The computing system of claim 61, wherein the first storage device and second storage device are operatively coupled to a single computer.

Claim 64 (Original): The computing system of claim 61, wherein the software application generates a cryptographic key as a function of the format information of the first storage device and decrypts the data of the second storage device using the generated key.

Claim 65 (Original): The computing system of claim 61, wherein the software application generates a cryptographic key as a function of the format information of the first storage device

PAGE 13/22 * RCVD AT 2/16/2004 3:10:12 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-2/0 * DNIS:7465447 * CSID:651 704 5951 * DURATION (mm-ss):07-14

and format information of the second storage device, and further wherein the software application decrypts the data of the second storage device using the generated key.

Claim 66 (Currently Amended): A computer comprising:

a storage drive operating in a read-only mode upon power-up[[,]];

a storage device operably coupled to the storage drive, wherein the storage device has device-specific format ~~security~~ information stored thereon; and

a storage manager to selectively configure the storage drive to operate in a read/write mode as a function of the ~~security~~ format information stored on the storage device.

Claim 67 (Original): The computer of claim 66, wherein the software application generates a cryptographic key as a function of the format information, verifies the security information on the storage device using the generated key and, upon verification, configures the storage drive to operate in read/write mode.

PAGE 14/22 * RCVD AT 2/16/2004 3:10:12 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-2/0 * DNIS:7465447 * CSID:651 704 5951 * DURATION (mm-ss):07-14